The “Classroom Problems” will be discussed and solved ex tempore at the tutorials in the same week as this problem set is handed out. These are intended to help you in getting started with the material, and will not yield any course credit.

The “Homework Problems” you should solve at home, and attend one of the tutorial sessions in the following week, prepared to present your solutions at class if requested. You earn one tutorial credit point (= 0.33 course points, for a maximum total of 6) for each of these problems that you have solved, and marked as solved at the tutorial session.

The “Demonstration Problems” illustrate further interesting aspects of the material. These will be discussed at the tutorials in the same week as the Homework Problems (time permitting) and printed solutions will be provided. You are encouraged to work on these, but no course credit is given for them.

Classroom problems:

1. Prove that if \( x \equiv x' \pmod{N} \) and \( y \equiv y' \pmod{N} \), then \( x \times y \equiv x' \times y' \pmod{N} \).

2. [Dasgupta et al., 1.25] Calculate \( 2^{125} \mod 127 \) using any method you choose.

Homework problems:

3. (a) [Dasgupta et al., 1.11] Is \( 4^{1536} - 9^{4824} \) divisible by 35?
   (b) [Dasgupta et al., 1.20] Find the inverse of: 20 mod 79; 3 mod 62; 21 mod 91; 91 mod 21
   (c) [Dasgupta et al., 1.22] Prove or disprove: If \( a \) has an inverse modulo \( b \), then \( b \) has an inverse modulo \( a \).

4. [Dasgupta et al., 1.34] On Lecture 13, slide 27 (Dasgupta et al. p. 29/37) it was claimed that since about a \( 1/n \) fraction of \( n \)-bit numbers are prime, the expected number of random \( n \)-bit numbers one needs to draw before hitting a prime is \( O(n) \). Verify this claim. (Hint: Suppose a particular coin has a probability \( p \) of coming up heads. How many times must you toss it, before it comes up heads? Method 1: Start by showing that the correct expression is \( \sum_{i=1}^{\infty} i(1-p)^{i-1}p \).
   Method 2: If \( E \) is the expected number of coin tosses, show that \( E = 1 + (1-p)E \).

5. Prove that when one is using universal hashing, the expected number of keys \( y \) colliding with a given fixed key \( x \) is less than 1. (Hint: Indicator random variables, linearity of expectation.)

Demonstration problems:

6. Prove that if \( p \) and \( q \) are distinct primes, then for every integer \( a \) and exponent \( e \) with \( e \neq 0 \pmod{(p-1)(q-1)} \), we have
   \[ a^e \equiv a^{e \mod{(p-1)(q-1)}} \pmod{pq}. \]

7. [Dasgupta et al., 1.43] In the RSA cryptosystem, user Alice’s public key \((N, e)\) is available to everyone. Suppose that her private key \( d \) is compromised and becomes known to eavesdropper Eve. Show that if \( e = 3 \) (a common choice), then Eve can efficiently factor \( N \). (Hint: Note that in the RSA cryptosystem, as described on Lecture 14, slide 9 (Dasgupta et al. p. 34/42), the primes \( p \) and \( q \) that make up \( N = pq \) are generated so as to be of the same length.)